(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11467 A2

(51) International Patent Classification[7]: H04Q 7/00

(21) International Application Number: PCT/GB01/03385

(22) International Filing Date: 27 July 2001 (27.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/626,700 27 July 2000 (27.07.2000) US

(71) Applicant *(for all designated States except US)*: **IPWIRELESS, INC.** [US/US]; 1250 Bayhill Drive, Suite 113, San Bruno, CA 94066 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JONES, William, John** [GB/GB]; Meadow Vale, Dauntsey, Chippenham SN15 4JH (GB). **BOWRING, Michael** [GB/GB]; Church Cottage, Bussage Hill, Bussage, Stroud GL6 8AY (GB). **WILLIAMS, Andrew, Gordon** [GB/GB]; 79 Ashford Road, Swindon SN1 3NT (GB).

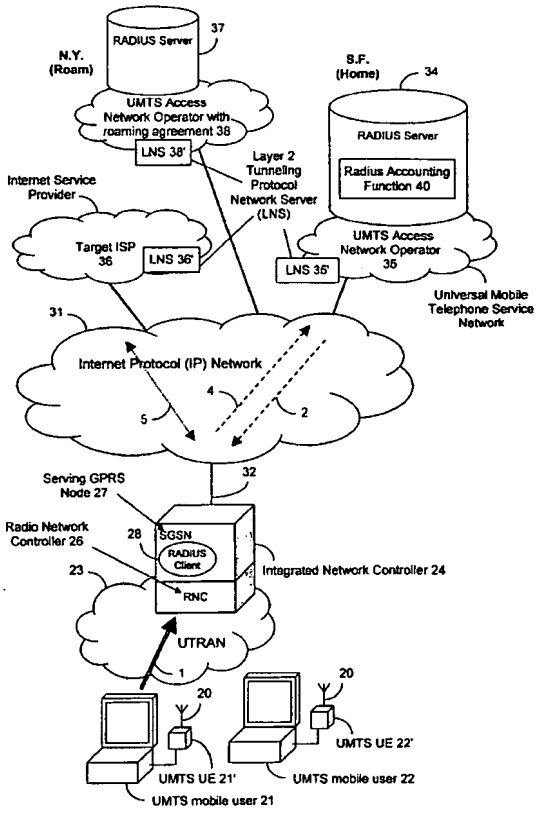
(74) Agent: **HUDSON, Peter**; InetIP, 121 Blackberry Lane, Four Marks, Alton, Hampshire GU34 5DJ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: USE OF RADIUS IN UMTS TO PERFORM HLR FUNCTION AND FOR ROAMING



(57) Abstract: Internet web technology is used, and specifically a RADIUS (Remote Authentication Dial-In User System) and associated protocols to authenticate network access for fixed end users and for end users who roam in a wireless system.

WO 02/11467 A2

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

USE OF RADIUS IN UMTS TO PERFORM HLR FUNCTION AND FOR ROAMING

RELATED APPLICATIONS

U.S. patent application Serial No. 09/626,582, filed July 27, 2000, entitled "USE OF INTERNET WEB TECHNOLOGY TO PERFORM ACCOUNTING FUNCTIONS", which is a continuation-in-part of U.S. patent application Serial No. 09/626,699, filed July 27, 2000, entitled "USE OF INTERNET WEB TECHNOLOGY TO REGISTER WIRELESS ACCESS CUSTOMERS," which is a continuation-in-part of U.S. patent application Serial No. 09/432,824, filed November 2, 1999, entitled "CELLULAR WIRELESS INTERNET ACCESS SYSTEM USING SPREAD SPECTRUM AND INTERNET PROTOCOL (IP)", and published in equivalent form as European patent publication EP1098539.

INTRODUCTION

The present invention is directed to the use of the Internet web technology to perform a home location register function in a wireless access network.

BACKGROUND OF THE INVENTION

As disclosed in application Serial No. 09/432,824 of November 2, 1999 entitled CELLULAR WIRE INTERNET ACCESS

SYSTEM USING SPREAD SPECTRUM AND INTERNET PROTOCOL (IP), this describes a cellular wireless Internet access system which operates in the 2 gigahertz or other frequency bands to provide high data rates to fixed and portable wireless Internet devices. Such users connect to near-by base stations which in turn communicate to Integrated Network Controllers which are then connected to the Internet. Such wireless implementation relates to an access network of the UMTS (Universal Mobile Telephone Service) and its subset UTRAN (Universal Terrestrial Radio Access Network) standards. UMTS/UTRAN standards are published by the 3G Project Partnership (3GPP), www.3gpp.org.

In any telecommunications access system, be it wired or wireless, there must be accommodation for end users who roam. In traditional cellular wireless systems, roaming is typically controlled by a Home Location Register (HLR) which communicates with the cellular network using traditional telecommunications protocols such as Signaling System #7 (SS7). Where the access to the Internet is via the Public Switched Telephone Network (PSTN), a RADIUS server provides such function. A description of RADIUS is provided by an Internet article, RFC2138 Remote Authentication Dial-In User Service (RADIUS) by C. Rigney, et al., April 1997 which is available at WWW.IETF.ORG (Internet Engineering Task Force). Thus far, this system, however, has only been used for Public Switched Telephone Network access.

Traditional mobile communications roaming methods protocols may not satisfactorily support the roaming function of the Internet Protocol (IP) based wireless access system describe in the above co-pending application 09/432,824. There is therefore a need for provision of HLR functions and roaming in an IP based wireless access system whereby the above disadvantages may be alleviated.

SUMMARY OF INVENTION

In accordance with a first aspect of the invention there is provided a method of operation in a wireless access network system, as claimed in claim 1.

In accordance with a second aspect of the invention there is provided a wireless access network system, as claimed in claim 13.

In accordance with a third aspect of the invention there is provided a RADIUS arrangement for use in a wireless access network system, as claimed in claim 25.

In accordance with a fourth aspect of the invention there is provided a network controller for use in a wireless access network system, the network controller having a RADIUS client for use with a RADIUS server in authorising user access to the network, as claimed in claim 26.

In accordance with a fifth aspect of the invention there is provided a computer program element comprising computer program means for performing the method of operation in a wireless access network system, as claimed in claim in claim 27.

In a preferred form of the invention, there is provided a method of operating a cellular wireless Internet access system using RADIUS (Remote Authentication Dial-In User Service) which is normally used for dial-up Internet access over the PSTN (Public Switched Telephone Network) where the user utilizes a portable subscriber terminal with a directly attached antenna for communicating in a wireless manner via a cellular network to an integrated network controller and then to a target Internet Service Provider (ISP), comprising the steps of providing the subscriber terminal with an access network operator identifier and user identifier and password, both related to said access network operator. The subscriber terminal requests Internet access from the integrated network controller. The integrated network controller requests verification of the user from the RADIUS server of the operator. The RADIUS server verifies the user identifier and password. The integrated network controller receives an acceptance message. The integrated network controller connects to a layer two tunneling protocol network server and a targeted Internet service provider and the subscriber terminal begins an Internet session.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an Internet system illustrating the present invention.

FIG. 2 is a flow chart illustrating the method of FIG. 1 of the present invention.

FIG. 3 is a diagram illustrating the method of FIG. 1 of the present invention.

FIG. 4 is a block diagram similar to FIG. 1.

FIG 5. is a flow chart for FIG. 4.

FIG. 6 is a data format diagram.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Referring now to FIG. 1, two typical users of the Internet access system are illustrated at 21 and 22. Each wireless access user has a personal computer PC and a UMTS user equipment (UE) 21' and 22' with a directly attached antenna 20 and is connected by typical data connections such as an RS232, USB or Ethernet to the PC. The user equipment is termed a portable subscriber terminal, operating in conjunction with its associated PC.

The wireless access user is described in the above co-pending application and is a part of a UMTS/UTRAN system 23 as described in the above co-pending application, which communicates in a wireless manner via a UTRAN network to an integrated network controller (INC) 24, via a link 1. Such controller may be connected by wire or otherwise to an Internet system or web 31. As discussed in the above co-pending application, the controller 24 includes an RNC or Radio Network Controller 26, which controls and allocates the radio network resources and provides reliable delivery of user traffic between a base station (NODE B) and subscriber terminal. An SGSN (Serving General Packet Radio Service Node) 27 provides session control. Lastly, a RADIUS element designated RADIUS client 28 is incorporated to provide authentication and other functions.

The Internet protocol network 31 is connected to INC 24 by an Internet Protocol connection 32 and then to a UMTS access network operator 35, through its Layer 2 Tunneling Protocol Network Server 35', having a RADIUS server 34. RADIUS server unit 34 may, for example, be in the user's home area of San Francisco (S.F.) and is the home Radius server. Thus, this is the server for both authentication and accounting functions as described in the above co-pending application. Thus, after authentication normally the user would communicate via the network 31 with target Internet service provider 36 through its Layer 2 Tunneling Protocol Network Server LNS 36'.

However, in the case where the user's subscriber terminal may be in New York (N.Y.), for example, he is a roaming user, who must use a partner access network operator. Specifically, RADIUS server 37 (N.Y.) along with a UMTS access network operator 38, which has a roaming agreement. Of course, that operator 38 would have an LNS unit 38'.

FIG. 2 illustrates the typical home operation of the system using RADIUS servers where after start as shown in step 1, the integrated network controller (INC) receives a session request from the mobile wireless user (UE) for Internet access. The numbered steps of FIG. 2 correspond to the communication paths illustrated in FIG. 1.

Next in step 2, INC 24 requests access verification for the mobile wireless user from the RADIUS server 34. Referring to FIG 1, for step 2 the link 2 is illustrated in network 31. In step 3, the decision is made by RADIUS server 34 whether to accept or reject the user as shown by the accept and reject paths and verifies the user ID and password. Each user, of course, has both a user identifier, a user password, and also includes an identification for its access network operator 35.

Thus, to summarize so far, when a user requests wireless Internet access, three pieces of authentication information are sent up into the network: 1) operator identifier - the name of the UMTS access licensed operator, 2) user identifier relating to the UMTS access

licensed operator, and 3) user password relating to the UMTS access licensed operator. As thus far illustrated, the user authentication is taking place within the home network. As will be discussed below, it can also take place where the user is roaming onto another network, as will be described in conjunction with FIGS. 4 and 5.

Completing the flow chart of FIG. 2, if the authentication is rejected as shown at 8, then in step 9, the INC 24 tears down the session and it comes to an end. However, if an acceptance takes place as shown in step 4, the integrated network controller receives the accept message (see the link 4 in the network 31 in FIG. 1) with the subscribed-to-tier of service, roaming indicator (in this case it would be negative) and target ISP. Then in step 5 (see the link 5 in FIG. 1) the INC 24 connects to the LNS 36' of the target ISP 36 and the user does an end-to-end negotiation for ISP access with LNS 36'. Then the Internet session, between the user's PC and the target ISP begins.

FIG. 3 illustrates the normal authentication, connection and session tear down between the INC radius client 28 and the home server 34. In step 41, access is requested and then accepted in 42. Then the connection is made as shown in 43 via a layer 2 tunneling protocol tunnel to the target ISP. Again, there is a disconnect access request at 44 and an access accept at 46. Finally, for accounting purposes a user disconnect notification is

provided to the radius server 34 as discussed in the above co-pending application.

FIG. 4 is very similar to FIG. 1 and simplified with the links 1, 2, 4, 5 being the same as illustrated in FIG. 1. Here, the user is attempting to gain access via UMTS roaming where access is desired with the partner or operator 38 with a roaming agreement.

Referring now to the flow chart of FIG. 5, as well as FIG. 4, after Start, in step 1 the INC 24 receives a session request from the wireless user as before. Then, in step 2 the INC 24 requests access verification for the mobile wireless user from the radius server 34. In this case, the access network operator identifier which has been supplied to the UE 21' and 22' is sent up via the radius client 28 and the SGSN 27 but identifies a different UMTS access network operator, with whom this operator has a roaming agreement. In other words, the users 21 and 22, as illustrated in FIG. 4, are now out of their home territory as shown by the access network operator ID. In step 3', the radius server 34 determines that this is a request from a roaming user (based on operator ID sent up in the request) and it forwards (link 3', FIG. 4) the request to the partner operator radius server 37. In decision step 3, the partner radius server 37 verifies user ID and password. If no verification occurs, then a rejection and tear down occurs as shown in steps 8 and 9 similar to FIG. 2.

However, if acceptance occurs then in step 10 via the link 10 as shown in FIG. 4 between partner operator 38 and home operator 35, the home radius server 34 receives the accept and passes it on to the INC 24. In step 4 and the link 4 shown in FIG. 4 (similar to that of FIG. 1) the INC 24 receives the accept message with the subscribed-to-tier of service, the roaming indicator (which in this case is positive), and the subscribed-to ISP. In step 5, as above, the INC 24 connects to the LNS of the target ISP 36. Again, the user begins a session.

To implement the above messages of FIG. 3 in RADIUS, the message types, structure and encoding are standard as outlined in the RFC 2138 above. As shown in those standards, the data packets all have pre-assigned attributes which are given a standard attribute number. To facilitate the additional functionality required for a RADIUS server to perform the HLR function, the standard attributes are required and also additional attributes. These are all contained in the code format of FIG. 6 where octets relate to the data octets and the box labeled TYPE relates to the attribute number. In the RADIUS system, attribute number 26 is a vendor-specific attribute. Morever, this is believed to be the most convenient way in order to interface with the standard RADIUS system. However, it is possible to create new attribute types. But it is believed that interfacing with the standard RADIUS system is the most efficient way to accomplish the method of the present invention. Thus, the following discussion relates to the message

definitions of FIG. 3 with the data format of FIG. 6 where when standard attributes must be used in a particular way they will be specifically described below.

FIG. 6 is a basic code format which would be modified for each particular function and, thus, it illustrates in general the basic code format. Now also referring to FIG. 3, with relation to step 41, the access request, a user name attribute is included (that is, type number 1) and the data of the octet string takes the form of a network access identifier (NAI) defined by an attribute number 32. For example, this might be user @ realm. Then, the vendor specific attribute (attribute number 26 as discussed above) which differentiates this system from the standard PSTN system would in the box of FIG. 6 labeled IPW-Type and have the number 10 to show a NODE B ID (that is, the base station ID). The identification of that ID would actually be in the VALUE box as shown in FIG. 6. Another vendor-specific attribute is the ISP name indicated in the IPW-Type box by the number 9, and the actual name would be expressed as a string octet as indicated in FIG. 6.

Next, with regard the step 42, the access-accept message, the present system provides a tier of service value which is related to the data capacity which the ultimate subscriber terminal is to have and also the latency. And latency, of course, is defined as a time lag between the beginning of a request for data and the moment it begins to be received. Thus, referring to FIG. 6 such tier of

service is indicated by IPW-Type attribute number 1 and in the value field the following enumerated values are provided starting from a low level to a high level.

0 Bronze
1 Silver
2 Gold
3 Business

In addition in the access accept message, there is another vendor-specific roaming indication indicating whether roaming is being done where in the value field of FIG. 6 after an IPW-Type number 2 is placed a value of 0 indicating a home network subscriber and a value of 1 indicating a roaming subscriber. Of course, the ISP name is also provided in a string data octet as discussed above. Lastly, there are no significant changes for either the access request or the access accept steps 44 and 46.

It is believed in the context of the wireless system as above that the assigning of tiers of services is unique especially when this is related to the standard data format of existing RADIUS standards.

It will, of course, be appreciated that the HLR and roaming functions discussed above will typically be carried out in computer programs or routines in software (like other system functions) running on processors (not shown).

Thus, an improved roaming function in a wireless network has been provided in which Radius Server and associated protocols replace the traditional UMTS or cellular network HLR function and its associated protocols.

WHAT IS CLAIMED IS:

1. A method of operation in a wireless access network system, comprising the steps of:

providing a RADIUS arrangement;

providing a network controller;

a user accessing the network via wireless user equipment and requesting access to a desired service provider;

the network controller receiving the user access request, requesting verification of the user from the RADIUS arrangement of the desired service provider and receiving user acceptance therefrom; and

the network controller connecting to the desired service provider and the user thereby establishing a communication link therewith to begin a communication session.

2. The method of claim 1, wherein a predetermined service provider identification is associated with the wireless user equipment and the step of requesting verification of the user comprises:

requesting verification of the user from a first RADIUS arrangement associated with a first service provider;

in the event that the predetermined service provider identification does not match that of the first service provider, the first RADIUS arrangement communicating the verification request to a further RADIUS arrangement of a service provider whose

identification matches the predetermined service provider identification; and

the further RADIUS arrangement communicating user acceptance to the network controller.

3. The method of claim 1 or 2, including assigning the user a tier of service value related to data capacity.

4. The method of claim 1, 2 or 3, including assigning the user a tier of service value related to latency.

5. The method of claim 3 wherein the assigned tier of service value is contained in a standard RADIUS format message.

6. The method of any preceding claim wherein the system is a cellular wireless Internet access system.

7. The method of any preceding claim wherein the system is a UMTS system.

8. The method of any preceding claim wherein a user identifier and password related to a predetermined service provider are associated with the wireless user equipment, and the step of requesting verification of the user comprises communicating the user identifier and password to the RADIUS arrangement of the desired service provider.

9. The method of any preceding claim wherein the step of the network controller connecting to the desired

service provider comprises the network controller connecting via a Layer 2 Tunneling Protocol link.

10. The method of any preceding claim wherein the service provider is an Internet service provider.

11. The method of any preceding claim wherein the step of requesting verification of the user comprises sending to the RADIUS arrangement a standard format RADIUS message containing:

a user name attribute,
a network access identifier equal to 32,
a vendor specific attribute equal to 26,
a base station ID value equal to 6,
a service provider value equal to 9, and
a text string indicating the name of the desired service provider.

12. The method of any preceding claim wherein the step of receiving user acceptance from the RADIUS arrangement of the desired service provider comprises receiving a standard format RADIUS message containing:

a user name attribute,
a network access identifier equal to 32,
a vendor specific attribute equal to 26,
a base station ID value equal to 6,
a service provider value equal to 9,
a text string indicating the name of the desired service provider, and
an indication of whether the user is a home network user or a roaming user.

13. A wireless access network system, comprising:

a RADIUS arrangement;

a network controller;

wireless user equipment for a user to access the network and to make a user access request to a desired service provider;

the network controller being arranged to receive the user access request, and to request verification of the user from the RADIUS arrangement of the desired service provider and to receive user acceptance therefrom; and

the network controller being arranged to connect to the desired service provider and the user thereby establishing a communication link therewith to begin a communication session.

14. The system of claim 13, wherein a predetermined service provider identification is associated with the wireless user equipment and

the network controller is arranged to request verification of the user by requesting verification of the user from a first RADIUS arrangement associated with a first service provider;

in the event that the predetermined service provider identification does not match that of the first service provider, the first RADIUS arrangement is arranged to communicate the verification request to a further RADIUS arrangement of a service provider whose identification matches the predetermined service provider identification; and

the further RADIUS arrangement is arranged to communicate user acceptance to the network controller.

15. The system of claim 13 or 14, wherein the system is arranged to assign the user a tier of service related to data capacity.

16. The system of claim 13, 14 or 15, wherein the system is arranged to assign the user a tier of service related to latency.

17. The system of claim 15 or 16 wherein a value indicative of the assigned tier of service is contained in a standard RADIUS format message.

18. The system of any one of claims 13-17 wherein the system is a cellular wireless Internet access system.

19. The system of any one of claims 13-18 wherein the system is a UMTS system.

20. The system of any one of claims 13-19 wherein a user identifier and password related to a predetermined service provider are associated with the wireless user equipment, and the network controller is arranged to request verification of the user by communicating the user identifier and password to the RADIUS arrangement of the desired service provider.

21. The system of any one of claims 13-20 wherein the network controller is arranged to connect to the desired service provider via a Layer 2 Tunnelling Protocol link.

22. The system of any one of claims 13-21 wherein the service provider is an Internet service provider.

23. The system of any one of claims 13-22 wherein the network controller is arranged to request verification of the user by sending to the RADIUS arrangement a standard format RADIUS message containing:

a user name attribute,
a network access identifier equal to 32,
a vendor specific attribute equal to 26,
a base station ID value equal to 6,
a service provider value equal to 9, and
a text string indicating the name of the desired service provider.

24. The system of any one of claims 13-23 wherein the RADIUS arrangement is arranged to indicate user acceptance to the network controller by sending a standard format RADIUS message containing:

a user name attribute,
a network access identifier equal to 32,
a vendor specific attribute equal to 26,
a base station ID value equal to 6,
a service provider value equal to 9,
a text string indicating the name of the desired service provider, and

an indication of whether the user is a home network user or a roaming user.

25. A RADIUS arrangement for use in a wireless access network system, the RADIUS arrangement being arranged to receive from a network controller of the system a request for verification of a wireless equipment user, and to provide to the network controller user acceptance.

26. A network controller for use in a wireless access network system, the network controller having a RADIUS client for use with a RADIUS server in authorising user access to the network.

27. A computer program element comprising computer program means for performing the method of operation in a wireless access network system as claimed in any one of claims 1 to 12.

28. A method of operating a cellular wireless Internet access system using RADIUS (Remote Authentication Dial-In User Service) which is normally used with a PSTN (Public Switched Telephone Network) where the user utilizes a portable subscriber terminal with a directly attached antenna for communicating in a wireless manner via a cellular network to an integrated network controller to a target Internet Service Provider (ISP), comprising the following steps:

providing said subscriber terminal with an access network operator identifier and user identifier and password, both related to said access network operator;

the subscriber terminal requesting access from the integrated network controller;

the integrated network controller requesting verification of the user from the RADIUS server of said operator;

the RADIUS server verifying the user identifier and password;

the integrated network controller receiving an acceptance message;

the integrated network controller connecting to a layer two tunneling protocol network server and a targeted Internet service provider and the subscriber terminal beginning an Internet session.

29. A method as in claim 28 including the step of said RADIUS server determining based on operator ID, that this is a roaming user, and the step of said RADIUS server of said home access network operator forwarding to a partner licensed operator and its said RADIUS server, the subscriber request for access, and the step of said partner RADIUS server verifying user ID and password and passing it on to the integrated network controller.

30. A method as in claim 28 including the step of assigning a subscriber terminal a tier of service value related to the data capacity and latency of said access system.

31. A method as in claim 28 where said RADIUS has a standard data format and including the step of storing said tier of service value in said format.

FIG. 1

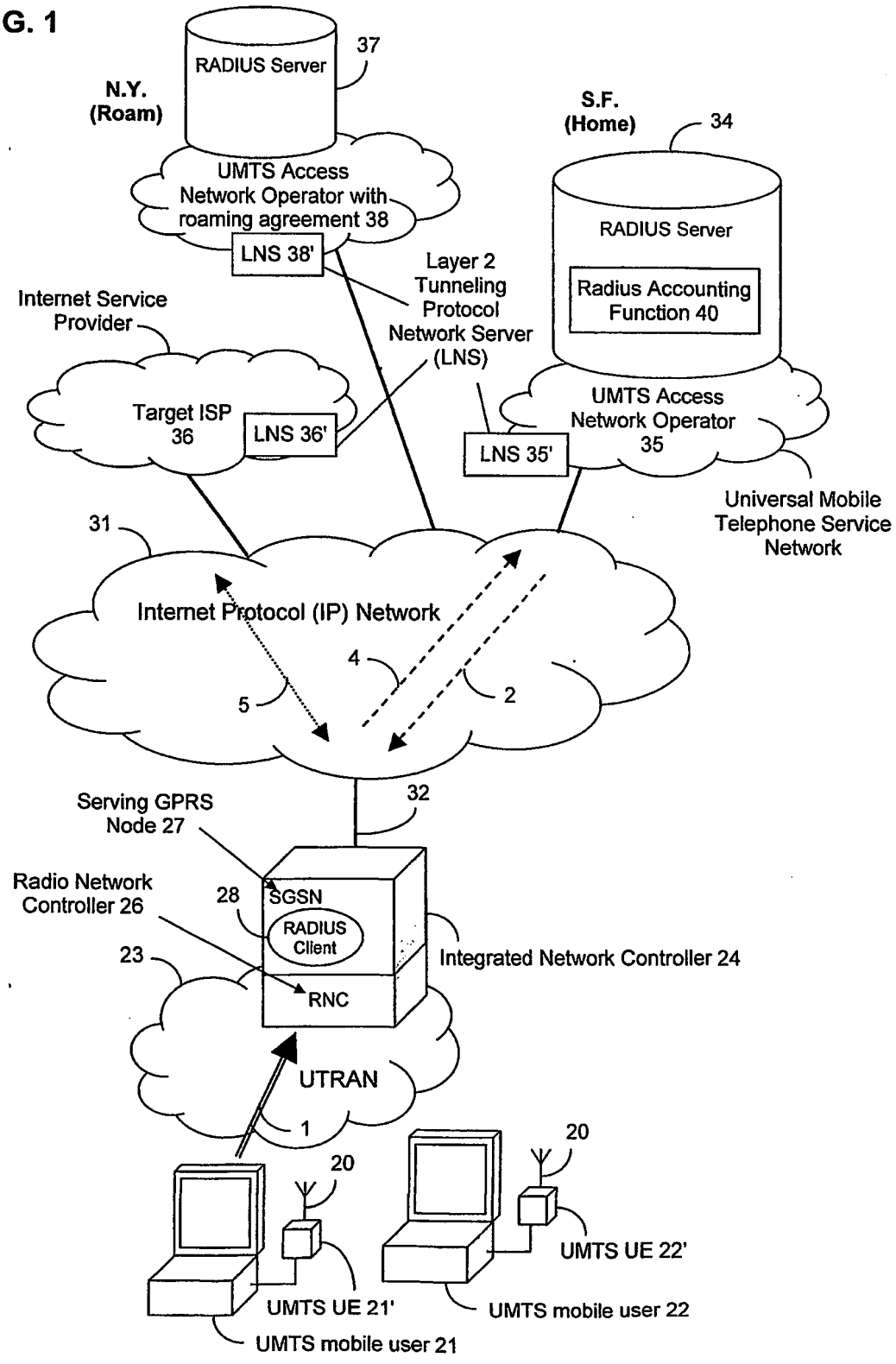
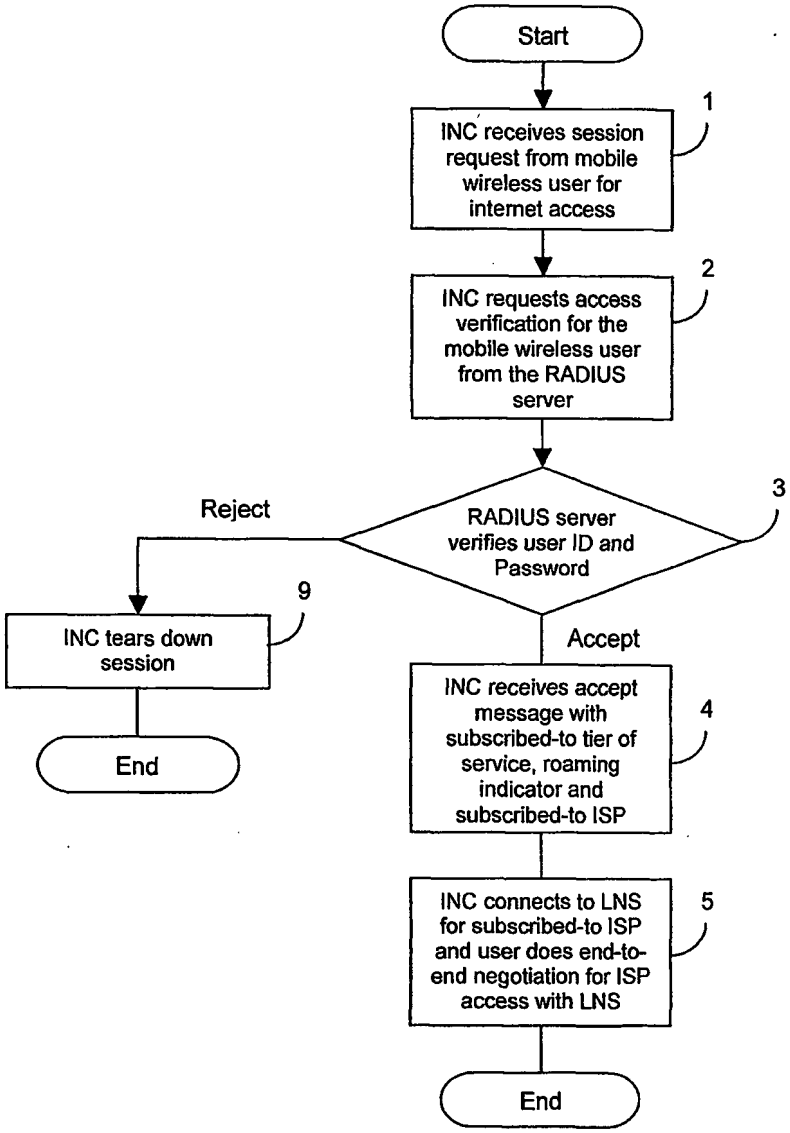

RADIUS Server
37
N.Y.
(Roam)
S.F.
(Home)
34
UMTS Access
Network Operator with
roaming agreement 38
LNS 38'
Layer 2
Tunneling
Protocol
Network Server
(LNS)
RADIUS Server
Radius Accounting
Function 40
Internet Service
Provider
Target ISP
36
LNS 36'
LNS 35'
UMTS Access
Network Operator
35
Universal Mobile
Telephone Service
Network
31
Internet Protocol (IP) Network
4
5
2
32
Serving GPRS
Node 27
Radio Network
Controller 26
28
SGSN
RADIUS
Client
23
RNC
Integrated Network Controller 24
UTRAN
1
20
20
UMTS UE 22'
UMTS UE 21'
UMTS mobile user 22
UMTS mobile user 21

FIG. 2


Start
INC receives session request from mobile wireless user for internet access
1
INC requests access verification for the mobile wireless user from the RADIUS server
2
RADIUS server verifies user ID and Password
3
Reject
Accept
INC tears down session
9
End
INC receives accept message with subscribed-to tier of service, roaming indicator and subscribed-to ISP
4
INC connects to LNS for subscribed-to ISP and user does end-to-end negotiation for ISP access with LNS
5
End

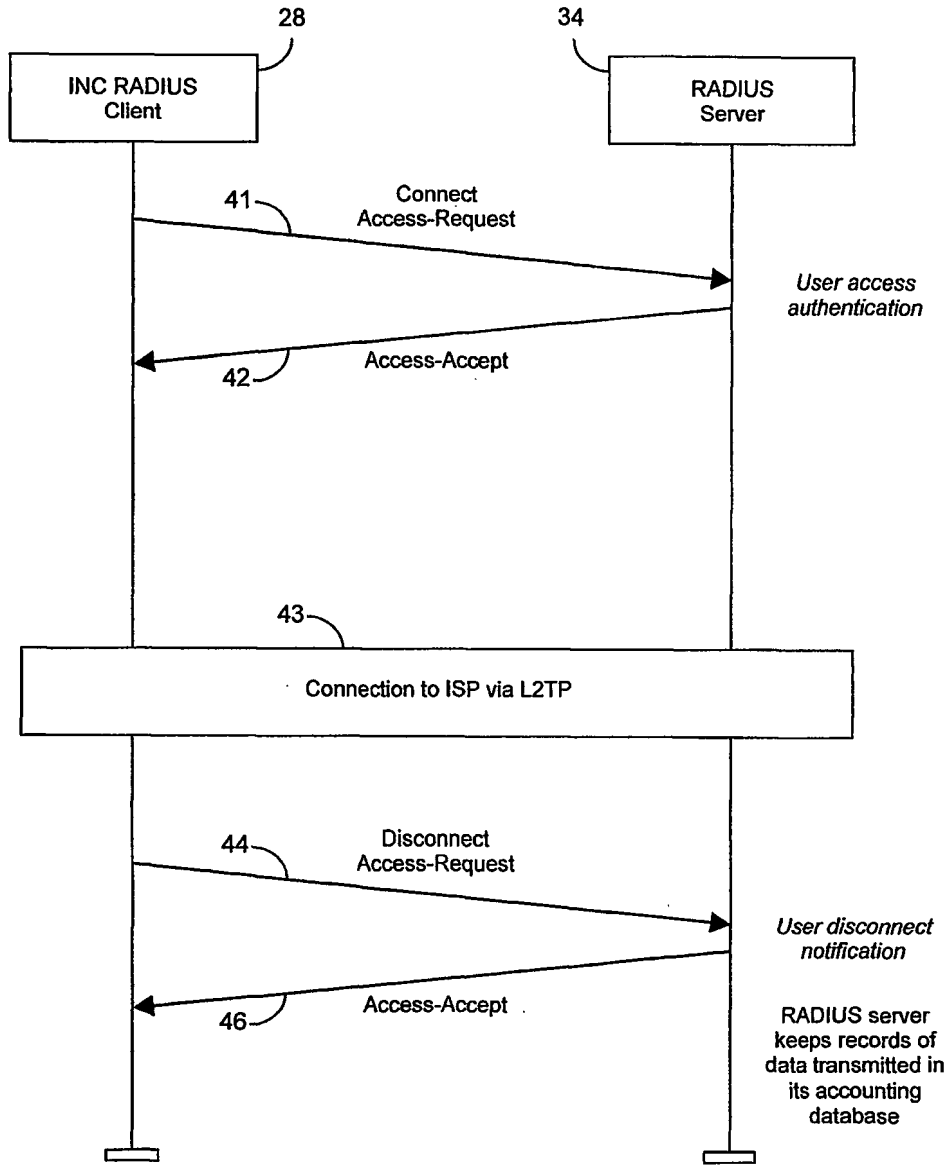

28
34
INC RADIUS Client
RADIUS Server
41
Connect Access-Request
User access authentication
42
Access-Accept
43
Connection to ISP via L2TP
44
Disconnect Access-Request
User disconnect notification
46
Access-Accept
RADIUS server keeps records of data transmitted in its accounting database

FIG. 3

FIG. 4

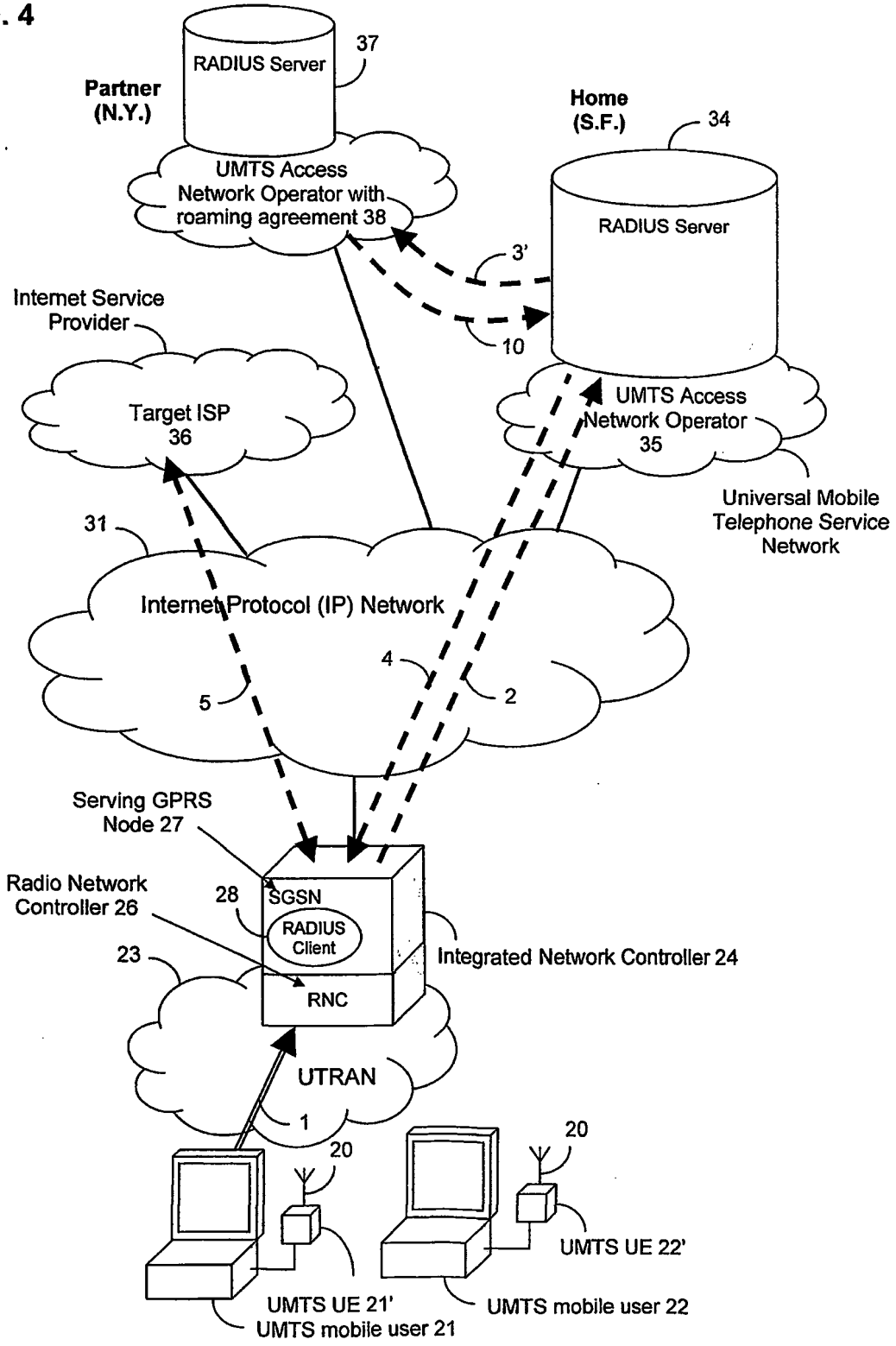

RADIUS Server
37
Partner
(N.Y.)
Home
(S.F.)
34
UMTS Access
Network Operator with
roaming agreement 38
RADIUS Server
3'
10
Internet Service
Provider
Target ISP
36
UMTS Access
Network Operator
35
Universal Mobile
Telephone Service
Network
31
Internet Protocol (IP) Network
4
2
5
Serving GPRS
Node 27
Radio Network
Controller 26
28
SGSN
RADIUS
Client
23
RNC
Integrated Network Controller 24
UTRAN
1
20
20
UMTS UE 22'
UMTS UE 21'
UMTS mobile user 21
UMTS mobile user 22

FIG. 5

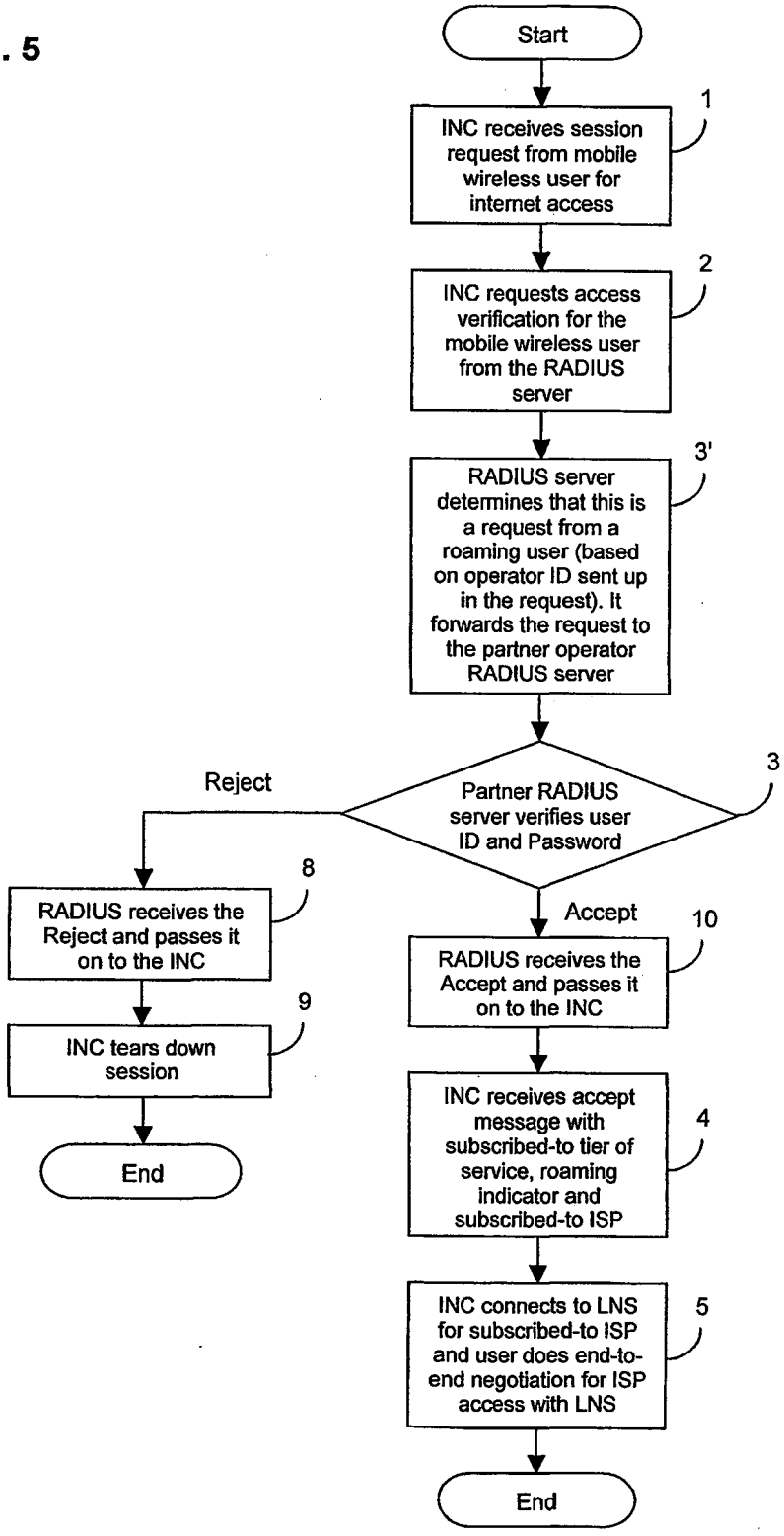
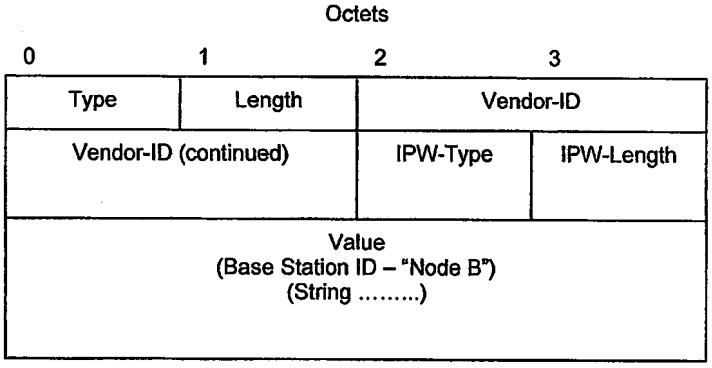

Start
1
INC receives session request from mobile wireless user for internet access
2
INC requests access verification for the mobile wireless user from the RADIUS server
3'
RADIUS server determines that this is a request from a roaming user (based on operator ID sent up in the request). It forwards the request to the partner operator RADIUS server
3
Partner RADIUS server verifies user ID and Password
Reject
8
RADIUS receives the Reject and passes it on to the INC
9
INC tears down session
End
Accept
10
RADIUS receives the Accept and passes it on to the INC
4
INC receives accept message with subscribed-to tier of service, roaming indicator and subscribed-to ISP
5
INC connects to LNS for subscribed-to ISP and user does end-to-end negotiation for ISP access with LNS
End

FIG. 6


Octets
0
1
2
3
Type
Length
Vendor-ID
Vendor-ID (continued)
IPW-Type
IPW-Length
Value
(Base Station ID – "Node B")
(String .....)